Authored by:

TLP:CLEAR
Product ID: AA23-201A
July 20, 2023

Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) is releasing this Cybersecurity Advisory to warn network defenders about exploitation of CVE-2023-3519, an unauthenticated remote code execution (RCE) vulnerability affecting NetScaler (formerly Citrix) Application Delivery Controller (ADC) and NetScaler Gateway. In June 2023, threat actors exploited this vulnerability as a zero-day to drop a webshell on a critical infrastructure organization's non-production environment NetScaler ADC appliance. The webshell enabled the actors to perform discovery on the victim's active directory (AD) and collect and exfiltrate AD data. The actors attempted to move laterally to a domain controller but network-segmentation controls for the appliance blocked movement.

The victim organization identified the compromise and reported the activity to CISA and Citrix. Citrix released a patch for this vulnerability on July 18, 2023.

This advisory provides tactics, techniques, and procedures (TTPs) and detection methods shared with CISA by the victim. CISA encourages critical infrastructure organizations to use the detection guidance included in this advisory for help with determining system compromise. If potential compromise is detected, organizations should apply the incident response recommendations provided in this CSA. If no compromise is detected, organizations should immediately apply patches provided by Citrix.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 13. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

To report suspicious or criminal activity related to information found in this Cybersecurity Advisory, contact CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Overview

In July 2023, a critical infrastructure organization reported to CISA that threat actors may have exploited a zero-day vulnerability in NetScaler ADC to implant a webshell on their non-production NetScaler ADC appliance. Citrix confirmed that the actors exploited a zero-day vulnerability: CVE-2023-3519. Citrix released a patch on July 18, 2023.[1]

CVE-2023-3519

CVE-2023-3519 is an unauthenticated RCE vulnerability affecting the following versions of NetScaler ADC and NetScaler Gateway:[1]

- NetScaler ADC and NetScaler Gateway 13.1 before 13.1-49.13
- NetScaler ADC and NetScaler Gateway 13.0 before 13.0-91.13
- NetScaler ADC and NetScaler Gateway version 12.1, now end of life
- NetScaler ADC 13.1-FIPS before 13.1-37.159
- NetScaler ADC 12.1-FIPS before 12.1-65.36
- NetScaler ADC 12.1-NDcPP before 12.65.36

The affected appliance must be configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or authentication, authorization, and auditing (AAA) virtual server for exploitation.[1]

CISA added CVE-2023-3519 to its Known Exploited Vulnerabilities Catalog on July 19, 2023.

Threat Actor Activity

As part of their initial exploit chain [T1190], the threat actors uploaded a TGZ file [T1105] containing a generic webshell [T1505.003], discovery script [TA0007], and `setuid` binary [T1548.001] on the ADC appliance and conducted SMB scanning on the subnet [T1046].

The actors used the webshell for AD enumeration [T1016] and to exfiltrate AD data [TA0010]. Specifically, the actors:

- Viewed NetScaler configuration files `/flash/nsconfig/keys/updated/*` and `/nsconfig/ns.conf` [T1005]. **Note:** These configuration files contain an encrypted password that can be decrypted by the key stored on the ADC appliance [T1552.001].
- Viewed the NetScaler decryption keys (to decrypt the AD credential from the configuration file) [T1552.004].
- Used the decrypted AD credential to query the AD via `ldapsearch`. The actors queried for:
  - Users (`objectClass=user`) (`objectcategory=person`) [T1087.002]
  - Computers (`objectClass=computer`) [T1018]
  - Groups (`objectClass=group`) [T1069.002]
  - Subnets (`objectClass=subnet`)
  - Organizational Units (`objectClass=organizationalUnit`)
  - Contacts (`objectClass=contact`)

  - Partitions (`objectClass=partition`)
  - Trusts (`objectClass=trustedDomain`) [T1482]

- Used the following command to encrypt discovery data collected via openssl in "tar ball" [T1560.001]: `tar -czvf - /var/tmp/all.txt | openssl des3 -salt -k <> -out /var/tmp/test.tar.gz`. (A "tar ball" is a compressed and zipped file used by threat actors for collection and exfiltration.)
- Exfiltrated collected data by uploading as an image file [T1036.008] to a web-accessible path [T1074]: `cp /var/tmp/test.tar.gz /netscaler/ns_gui/vpn/medialogininit.png`.

The actors' other discovery activities were unsuccessful due to the critical infrastructure organization's deployment of their NetScaler ADC appliance in a segmented environment. The actors attempted to:

- Execute a subnet-wide curl command to identify what was accessible from within the network as well as potential lateral movement targets.
- Verified outbound network connectivity with a ping command (`ping -c 1 google.com`) [T1016.001].
- Executed host commands for a subnet-wide DNS lookup.

The actors also attempted to delete their artifacts [TA0005]. The actors deleted the authorization configuration file (`/etc/auth.conf`)—likely to prevent configured users (e.g., admin) from logging in remotely (e.g., CLI) [T1531]. To regain access to the ADC appliance, the organization would normally reboot into single use mode, which may have deleted artifacts from the device; however, the victim had an SSH key readily available that allowed them into the appliance without rebooting it.

The actors' post-exploitation lateral movement attempts were also blocked by network-segmentation controls. The actors implanted a second webshell on the victim that they later removed. This was likely a PHP shell with proxying capability. The actors likely used this to attempt proxying SMB traffic to the DC [T1090.001] (the victim observed SMB connections where the actors attempted to use the previously decrypted AD credential to authenticate with the DC from the ADC via a virtual machine). Firewall and account restrictions (only certain internal accounts could authenticate to the DC) blocked this activity.

MITRE ATT&CK TACTICS AND TECHNIQUES

See Table 1–Table 9 for all referenced threat actor tactics and techniques in this advisory.

Table 1: Cyber Threat Actors ATT&CK Techniques for Initial Access

Technique Title	ID	Use
Exploit Public-Facing Application	T1190	The threat actors exploited CVE-2023-3519 to implant a webshell on the organization's NetScaler ADC appliance.

Table 2: Cyber Threat Actors ATT&CK Techniques for Persistence

Technique Title	ID	Use
Server Software Component: Web Shell	T1505.003	The threat actors implanted a generic webshell on the organization's NetScaler ADC appliance.

Table 3: Cyber Threat Actors ATT&CK Techniques for Privilege Escalation

Technique Title	ID	Use
Abuse Elevation Control Mechanism: Setuid and Setgid	T1548.001	As part of their initial exploit chain uploaded a TGZ file contain a `setuid` binary on the ADC appliance.

Table 4: Cyber Threat Actors ATT&CK Techniques for Defense Evasion

Technique Title	ID	Use
Masquerading: Masquerade File Type	T1036.008	The threat actors exfiltrated data by uploading it as an image file to a web-accessible path.

Table 5: Cyber Threat Actors ATT&CK Techniques for Credential Access

Technique Title	ID	Use
Unsecured Credentials: Credentials In Files	T1552.001	The threat actors obtained encrypted passwords from NetScaler ADC configuration files, and the decryption key was stored on the ADC appliance.
Unsecured Credentials: Private Keys	T1552.004	The threat actors obtained decryption keys to decrypt the AD credential obtained from the NetScaler ADC configuration files.

Table 6: Cyber Threat Actors ATT&CK Techniques for Discovery

Technique Title	ID	Use
Domain Trust Discovery	T1482	The threat actors queried the AD for trusts.
Permission Groups Discovery: Domain Groups	T1069.002	The threat actors quired the AD for groups.
Remote System Discovery	T1018	The threat actors queried the AD for computers. The threat actors attempted to execute a subnet-wide curl command to identify what was accessible from within the network as well as potential lateral movement targets. Network-segmentation controls prevented this activity.
System Network Configuration Discovery	T1016	The actors used a webshell for AD enumeration.
System Network Configuration Discovery: Internet Connection Discovery	T1016.001	The threat actors attempted to verify outbound network connectivity with a ping command and executed host commands for a subnet-wide DNS lookup. Network-segmentation controls prevented this activity.

Network Service Discovery	T1046	The threat actors conducted SMB scanning on the organization's subnet.
Account Discovery: Domain Account	T1087.002	The threat actors queried the AD for users.

Table 7: Cyber Threat Actors ATT&CK Techniques for Collection

Technique Title	ID	Use
Archive Collected Data: Archive via Utility	T1560.001	The threat actors encrypted discovery data collected via openssl in "tar ball."
Data from Local System	T1005	The threat actors viewed NetScaler ADC configuration files `flash/nsconfig/keys/updated/*` and `/nsconfig/ns.conf`.
Data Staged	T1074	The threat actors uploaded data as an image file to a web-accessible path: `cp /var/tmp/test.tar.gz /netscaler/ns_gui/vpn/medialogininit.png`.

Table 8: Cyber Threat Actors ATT&CK Techniques for Command and Control

Technique Title	ID	Use
Ingress Tool Transfer	T1105	The threat actors exploited CVE-2023-3519 to upload a TGZ file containing a generic webshell, discovery script, and `setuid` binary on the ADC appliance.
Proxy: Internal Proxy	T1090.001	The actors likely used a PHP shell with proxying capability to attempt proxying SMB traffic to the DC (the traffic was blocked by a firewall and account restrictions).

Table 9: Cyber Threat Actors ATT&CK Techniques for Impact

Technique Title	ID	Use
Account Access Removal	T1531	The threat actors deleted the authorization configuration file (`/etc/auth.conf`)—likely to prevent configured users from logging in remotely (e.g., CLI).

DETECTION METHODS

Run the following victim-created checks on the ADC shell interface to check for signs of compromise:

1. Check for files newer than the last installation.
2. Modify the `-newermt` parameter with the date that corresponds to your last installation:
   - `find /netscaler/ns_gui/ -type f -name *.php -newermt [YYYYMMDD] -exec ls -l {} \;`
   - `find /var/vpn/ -type f -newermt [YYYYMMDD] -exec ls -l {} \;`
   - `find /var/netscaler/logon/ -type f -newermt [YYYYMMDD] -exec ls -l {} \;`
   - `find /var/python/ -type f -newermt [YYYYMMDD] -exec ls -l {} \;`
3. Check http error logs for abnormalities that may be from initial exploit:
   - `grep '\.sh' /var/log/httperror.log*`
   - `grep '\.php' /var/log/httperror.log*`
4. Check shell logs for unusual `post-ex` commands, for example:
   - `grep '/flash/nsconfig/keys' /var/log/sh.log*`
5. Look for `setuid` binaries dropped:
   - `find /var -perm -4000 -user root -not -path "/var/nslog/*" -newermt [YYYYMMDD] -exec ls -l {} \;`
6. Review network and firewall logs for subnet-wide scanning of HTTP/HTTPS/SMB (80/443/445) originating from the ADC.
7. Review DNS logs for unexpected spike in internal network computer name lookup originating from the ADC (this may indicate the threat actor resolving host post-AD enumeration of computer objects).
8. Review network/firewall logs for unexpected spikes in AD/LDAP/LDAPS traffic originating from the ADC (this may indicate AD/LDAP enumeration).

9. Review number of connections/sessions from NetScaler ADC per IP address for excessive connection attempts from a single IP (this may indicate the threat actor interacting with the webshell).
10. Pay attention to larger outbound transfers from the ADC over a short period of session time as it can be indicative of data exfiltration.
11. Review AD logs for logon activities originating from the ADC IP with the account configured for AD connection.
12. If logon restriction is configured for the AD account, check event `4625` where the failure reason is "User not allowed to logon at this computer."
13. Review NetScaler ADC internal logs (`sh.log*`, `bash.log*`) for traces of potential malicious activity (some example keywords for `grep` are provided below):
    - `database.php`
    - `ns_gui/vpn`
    - `/flash/nsconfig/keys/updated`
    - `LDAPTLS_REQCERT`
    - `ldapsearch`
    - `openssl + salt`
14. Review NetScaler ADC internal access logs (`httpaccess-vpn.log*`) for 200 successful access of unknown web resources.

INCIDENT RESPONSE

If compromise is detected, organizations should:

1. Quarantine or take offline potentially affected hosts.
2. Reimage compromised hosts.
3. Provision new account credentials.
4. Collect and review artifacts such as running processes/services, unusual authentications, and recent network connections.
5. Report the compromise to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870).

MITIGATIONS

CISA recommends all organizations:

- **Install the relevant updated version of NetScaler ADC and NetScaler Gateway** as soon as possible. See Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467 for patch information.
- **Follow best cybersecurity practices** in your production and enterprise environments, including mandating phishing-resistant multifactor authentication (MFA) for all staff and for all services. For additional best practices, see CISA's Cross-Sector Cybersecurity Performance Goals (CPGs). The CPGs, developed by CISA and the National Institute of Standards and Technology (NIST), are a prioritized subset of information technology (IT) and operational technology (OT) security practices that can meaningfully reduce the likelihood and impact of known cyber risks and common TTPs. Because the CPGs are a subset of best practices, CISA and ACSC also recommend software manufacturers implement a comprehensive information security program based on a recognized framework, such as the NIST Cybersecurity Framework (CSF).
- As a longer-term effort, **apply robust network-segmentation controls on NetScaler appliances**, and other internet-facing devices.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, CISA recommends exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. CISA recommends testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Table 1–Table 9).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

CISA recommends continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

REFERENCES

[1] Citrix Security Bulletin CTX561482: Citrix ADC and Citrix Gateway Security Bulletin for CVE-2023-3519, CVE-2023-3466, CVE-2023-3467